An Analytical Approach To Analyze The Impact Of Gray Hole Attacks In Manet

Usha G[1], Bose S[2],
[1]Department of Computer Science and Engineering, Anna University, Chennai
Email: ushag2@gmail.com
[2]Department of Computer Science and Engineering, Anna University, Chennai
Email: sbs@cs.annauniv.edu

***Abstract*— Mobile adhoc networks are connected by wireless links which forms a random topology of mobile nodes.Random topology and self-organising network provides on-demand networking and dynamic topology.Due to lack of infrastructure support each node are self-organising and any nodes can join and leave the network at any time.Providing security to these network is a challenging issue because these type of networks suffer for various kinds of malicious attacks.One of the attacks which are most difficult to detect in Mobile adhoc network is Gray hole attack.In this paper an analytical Gray Hole attack model is developed for AODV protocol.Experiments are simulated for Gray Hole attacks under variety of adhoc network condition.**

***Index Terms*—AODV,Gray Hole attack,Mobile Adhoc Netorks(MANET),packet delivery ratio,security**

I. Introduction

Mobile adhoc network security[1][2] is very difficult and important task.Because of the dynamic topology each and every layer in MANET suffers for various kinds of attacks[3].The applications of Manets include in business meetings,battlefield,interactive conferences,hurricane ,earthquake and other applications like personal area networking,sensor networks,mesh networks etc..In mobile adhoc networks because of dynamic routing frequent topology changes.In MANET routing involves three types of approaches,they are proactive approach, reactive approach,hybrid approach. AODV protocol is one of the on-demand routing protocol and widely used in MANET routing.AODV protocol [4] uses the sequence number to find the latest route to the destination.

Routing layer in MANET's suffers for various types of attacks [5] [6] [7] [8]..The malicious node sabotage the other nodes or the whole network by dropping the packets. Hence,the Gray hole attack is one such type of attack, in which the malicious node drops the packets with certain probability i.e., It drops all the packets or either drop few packets.For analytical modeling first order logic is used.In order to analyze the network performance the key attributes such as packet delivery ratio,packet drop ratio,normalized routing load,overhead are used.In this paper the performance of AODV protocol is analysed based on the above attributes.The remainder of the paper is organized as follows; Section II discusses about AODV protocol and its vulnerability.Section III discusses about gray hole attack in detail. Section IV discusses simple analytical model for gray hole attack. In section V, discusses proposed framework for analyzing the attack in detail. Section VI discusses about simulation environment and discussed about results. Finally section VII concludes this paper and discussed about future work.

II. AODV Protocol and Its Vulnerabilities

AODV protocol is a routing protocol which are type of demand-driven protocols.Before understanding the vulnerable behavior of the protocol ,understanding the working of the protocol is important

A. Basic Working of AODV Protocol

AODV [9] is known as on-demand because it invokes only when a node has data to transmit.It uses IP addressing and uses UDP as the transport layer protocol which offers either error recovery or flow control.The Figure.1.illustrates the message formats of RREQ and RREP and also discusses about the normal communication between source and destination. As shown in Figure.1.AODV protocol contains the set of messages,like RREQ-Route Request,RREP-Route Reply additionally they have the messages such as RERR-Route Error,HELLO-For link status monitoring.A RREQ message is broadcasted when a node wants to transmit or communicate with other nodes.RREQ message propagates through the network which also contains a recent sequence number for the destination.So a valid destination route has a sequence number at least as great as that contained in RREQ.When a RREQ message reaches a destination node it generates a RREP message only if it is itself the destination,it has an active route to the destination.

B. Vulnerability of AODV Protocol

AODV protocol is more [10] vulnerable. In this paper misuse of the RREP message i.e,"Send Fake RREP" message by destination is focused.The basic analytical approach for analyzing this attack is discussed in section VI.For AODV Protocol the intruder either drops the packets,modifies the message formats and then forwards,the attacker sends a faked message for the received routing message or finally the attacker sends a faked message with out any intention.

III. Gray Hole Attack in Detail

A Gray hole node[11] exhibit a behavior which is a combination of the above two, thereby making its detection

DOI: 03.LSCS.2013.1.532

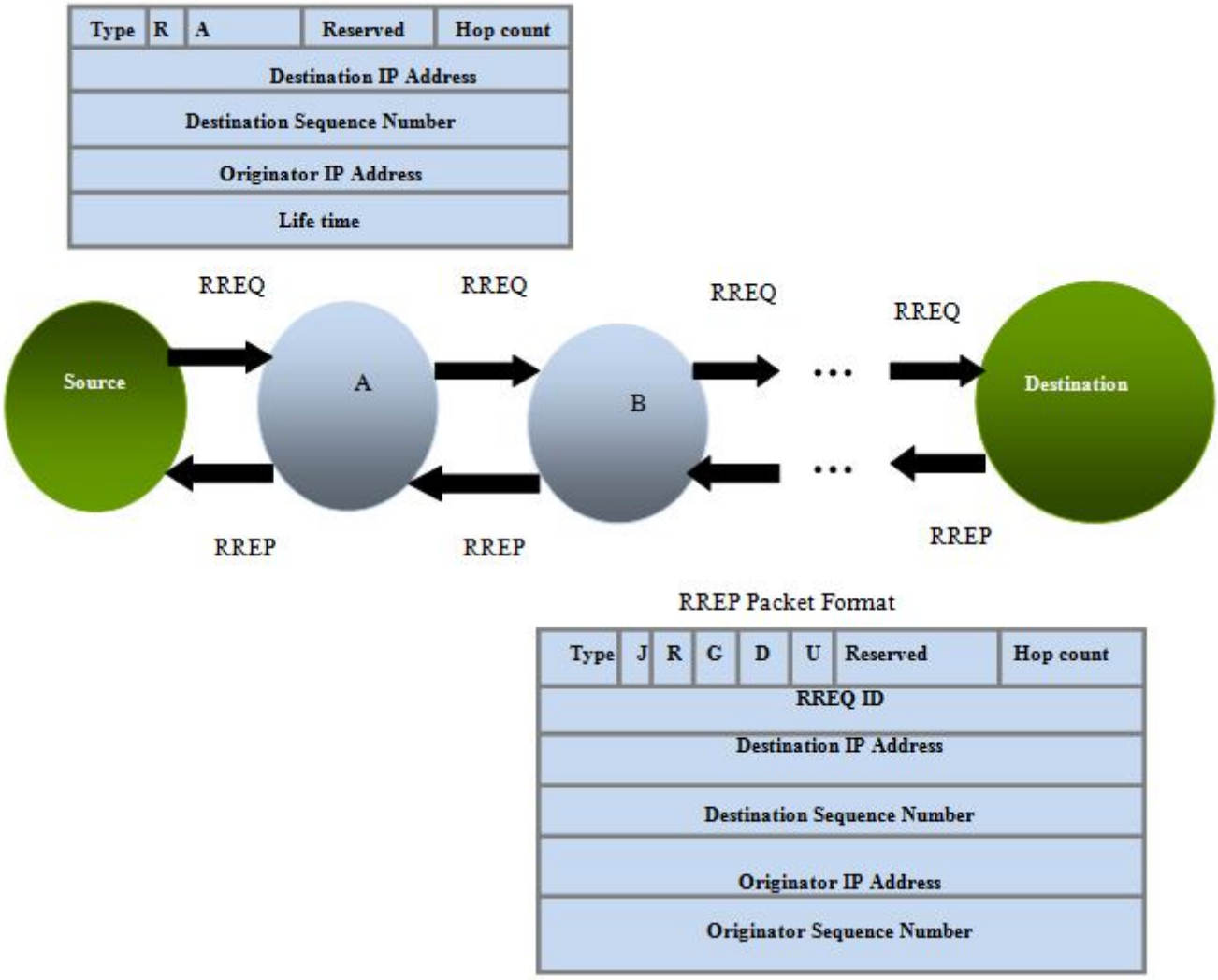

Fig. 1. AODV working with RREQ and RREP messages and its message format

even more difficult. For example whenever the source node wants to transmit data to Destination node,the source node initially broadcasts a Route request (RREQ) packets to its neighbors in order to find a fresh route to the desired destination. The neighbor nodes checks to see in its routing table whether it is the destination or it has the route to destination. When the malicious node overhears this information it indicates that it has the fresh route to the destination (i.e., highest sequence number).

IV. Analytical Model

In this section, an analytical approach towards Gray Hole attack against the AODV protocol is discussed. The following are details on how a malicious node can launch gray hole attack in the network.Let us take a Mobile adhoc network consist of set of edges and vertices denoted using a graph G={V,E}.The normal nodes are represented using the set{N},the malicious gray hole nodes can be denoted as {G},in other words using FOL it can be represented using Normal Node (N), Gray Hole Node (G).

In Mobile adhoc network let us take there exist some gray hole node which can be denoted as

$$\exists\ g(\text{Grayhole}(G)) \quad (1)$$

So the network consist of set of nodes which consist of adjoining normal node and malicious nodes

$$\forall S\ \text{Manet}(s) \Leftrightarrow (s=\{\text{Normalnode}(n)\} \vee \exists g,s2\ (\text{Grayhole node}\ (G) \wedge s=\{x/s2\}) \quad (2)$$

In order to conduct packet drop attack a Gray hole node in manet drops packets coming from or destined to specific nodes.

$$\forall d\text{Packet drop}(d) \Leftrightarrow (S=\{\ \exists g\ \text{Grayholenode}\ (G)\}) \vee (\exists z,S2\ ,\text{Set(Forward Packet to other nodes(S2)} \wedge S=\{z/s2\})) \quad (3)$$

For some time duration Gray Hole nodes drop packets but later switch to behave normally .

$$\forall d\ \text{Packet drop}(d) \Rightarrow \exists g\ \text{Grayhole}(T,d) \wedge \text{Switchto normal}(T) \quad (4)$$

Thus first order logic is used to depict the attack scenario in MANET environment

V. Proposed Framework For Gray Hole Attack Analysis

A simple framework for generating Gray Hole attack is

DOI: 03.LSCS.2013.1.532

proposed in this section.It has two phases

- Initial Phase
- Attacking Phase

In the initial phase the incoming packets are checked to see whether they belong to AODV packets and further the packets are checked whether they belong to RREQ type of packets.If so,in Attacking phase the attacker increases the sequence number of the RREP packets.For example,when a source node receives fakeRREP message it updates its routing table towards non-existing (malicious) node. In the simulation "send Fake RREP" to the source node at a particular frequency of malicious node is considered .It can be achieved by an increasing destination sequence number and reducing hop count. The following Fig.2. illustrates this simple framework for generating Gray hole attack in MANET.

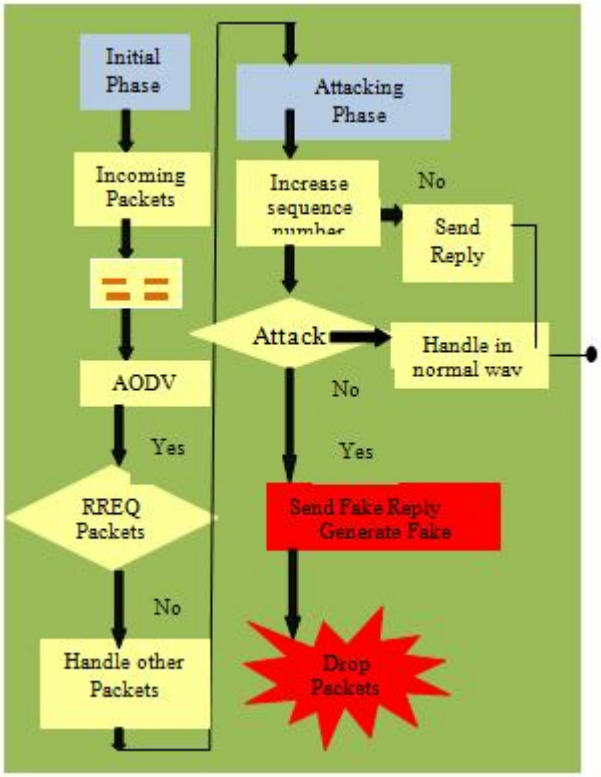

Fig. 2. Simple Framework for generating GrayHole Attacks

VI. Simulation Environment

As discussed above for the simulation NS-2 [12] is used for evaluation. Evaluations are based on the simulation of 60 wireless mobile nodes that forms a mobile adhoc network over a rectangular (600 m X 600 m) grid. The MAC layer protocol used in the simulation is IEEE 802.11. 0% to 40% of nodes are selected as malicious nodes. Various network densities from 20%, 30%, 40%, 50%, and 60% are tried. Table I, Table II, Table III lists the parameter settings for a simulation environment

A.Traffic and Mobility Model

The trails used were constant bit rate (CBR). Each node transmits 512 bytes of data packets at a certain rate (packets/ second). The transport agent used was UDP.For each set of

Table I. MANET Environment

Property	Value
Channel type	Wireless Channel
Propagation Model	Two ray ground
Antenna type	Omni Antenna
Interface Queue typeDrop	Tail/PriQueue
MAC Type	802.11
Maximum Packets in Queue	50
Topological Area	600m X 600 m
Mobility Scenario	10 m/s
Pause time	20 Sec
Mobility Model	Random way point

parameters; Each simulation is repeated for 3 times and calculated the average of the results. The simulation is run for 15 times for normal AODV with 5 different numbers of network sizes and three repetitions are considered . So for 5 different numbers of network size with gray hole attack and 4 different numbers of nodes (malicious) , the gray hole simulation was run for 40 times. And it was repeated for 3 times and makes it as 120 runs.

Table II. Traffic Parameters for Simulation

Property	Values
Traffic Agent	CBR
Transport Agent	UDP
Traffic Source	7
Traffic Sink	7
CBR rate	10 Kbytes/s

Table III.Variable Parameters for Simulation

Property	Values
Routing Protocol	Normal AODV
AODV with GrayHole	Number of Gray Holes1,2,3,4.
Number of nodes	20,30,40,50,60.

So the following results in section 6 were then prepared from the output of 135 simulation runs. Different network scenarios are (20, 30, 40, 50 and 60 Nodes)used to run the simulation. The scenario generator available in ns2 which is used for generating 5 x 3 scenarios (for three repetitions). Above tables discuss the various parameters for the simulation.Some movements in the scenario are also introduced.

1.Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the CBR sources is known as packet delivery fraction.

Packet Delivery Fraction=D_r/D_t

Where Dr is the number of data packets successfully received and is the number of data packets transmitted.

2.Normalized Routing Load

Normalized routing load is the ratio between the total numbers of packets transmitted from routing layer of the source to the total number of packets received at the application layer of the destination.

3. Total Dropped Packets

Packets drop value is calculated because the packet drop occurs due to any reason as a performance metric. Packet

DOI: 03.LSCS.2013.1.532

drop is used to detect packet drop anomaly.

4.Overhead

Here the overhead is measured in terms of total generated routing packets. It is the count of total packet generated and forward at the network layer. In the following table, all the measured values in the case of Normal AODV protocol are tabulated.

5.Simulation Results

Now in this section simulation results are discussed based on the attributes such as packet delivery fraction,normalized routing load,dropped packets,overhead.

6.Packet Delivery Fraction

A packet delivery ratio is a standard measure of throughput. Packet delivery ratio for normal AODV and AODV with the gray hole attack is presented . In general without malicious node AODV have got a good packet delivery ratio The results are presented for AODV in the absence of malicious nodes in Figure 3. In table IV, it shows the performance of normal AODV based on various node densities.

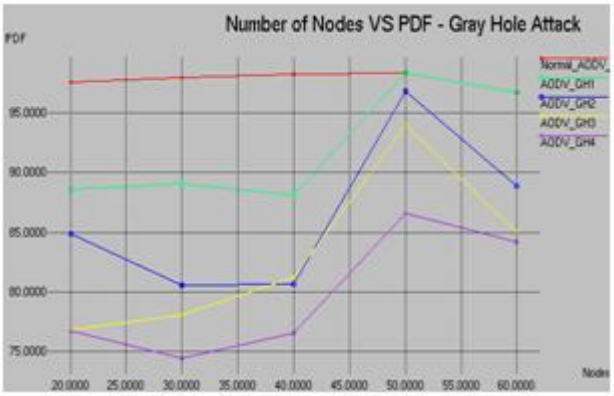

Fig. 3. Number of Nodes vs. Packet delivery fraction

TABLE IV. ANALYSIS ON NORMAL AODV

Protocol	Nodes	PDF	NRL	Routing Packets	Dropped
AODV	20	97.60	0.38	620.33	73
	30	97.97	0.61	1008.67	65
	40	98.30	0.65	1079.67	43
	50	98.40	0.73	1206.67	38
	60	96.77	1.46	2399.00	87

7. Normalized Routing Load

The normalized Routing load can be evaluated based on messages like RREQ and RREP with the statistics of number of routed packets to that of received packets. The following Figure. 4 explains about normalized routing load in the presence and absence of malicious nodes.

8. Dropped Packets

This metric not identifies other reasons for packet loss,

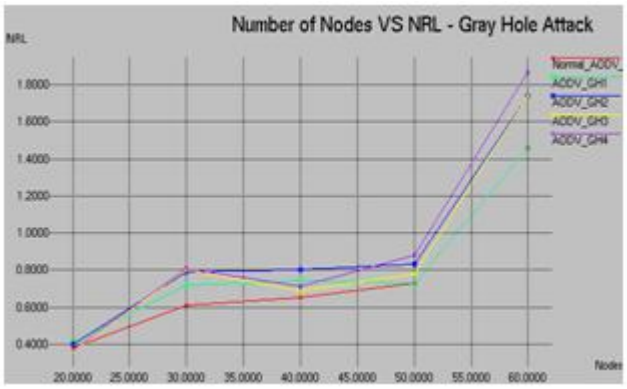

Fig. 4. Number of Nodes vs. Normalized Routing Load

but it is useful towards detecting packet dropped attacks.The following Figure 5 illustrates about number of nodes vs dropped packets.

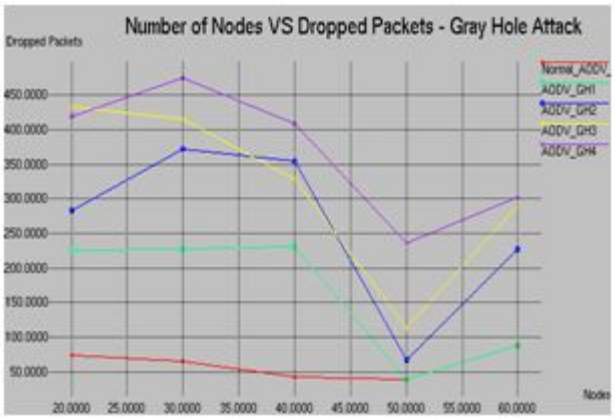

Fig. 5. Number of Nodes vs. Dropped Packets

9. Overhead

Overhead is the useful metric for analyzing extra bandwidth consumed to deliver data packets.Figure 6 discusses about the overhead in the network due to the Gray Hole Attack

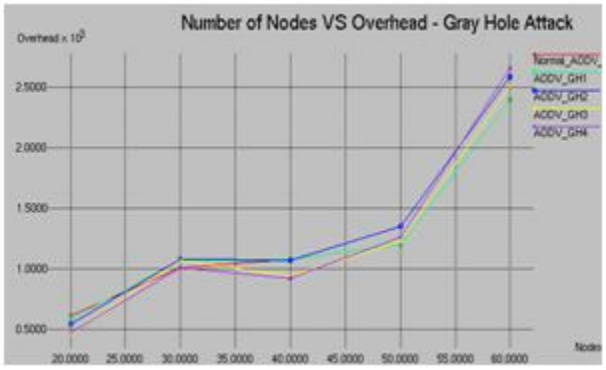

Fig. 6. Number of Nodes vs. Overhead

The following Table 6 illustrates the details about the analysis results of Gray hole attacks under various network environments such as packet delivery ratio,normalized routing load,routing packets,dropped packets.Packet delivery ratio decreases with increasing node densities and percentage of Gray hole nodes.As shown in Figure 4 no constant trend is observed.When the number of Grayhole nodes gets increased

DOI: 03.LSCS.2013.1.532

the normalized routing load also increased.While in the case of dropped packets ,packet drop count increases with increasing node densities of Gray hole nodes.Finally the overhead in the network is also increased in the presence of Gray hole nodes.

TABLE VI. ANALYSIS ON AODV WITH GRAY HOLE ATTACK

Protocol	Nodes	PDF	NRL	Routing Packets	Dropped
With Gray Hole 1	20	88.57	00.41	595.00	226
	30	89.10	00.72	1075.00	227
	40	88.13	00.74	1084.67	231
	50	98.40	00.73	1206.67	38
	60	96.77	10.46	2399.00	87
With Gray Hole 2	20	84.83	0.40	551.33	283
	30	80.57	0.79	1083.00	373
	40	80.70	0.80	1076.00	355
	50	96.87	0.83	1357.00	67
	60	88.87	1.74	2594.00	227
With Gray Hole 3	20	76.80	0.36	465.00	434
	30	78.07	0.80	1070.67	415
	40	81.23	0.69	941.00	329
	50	94.00	0.78	1233.00	113
	60	85.03	1.74	2516.00	291
With Gray Hole 4	20	76.70	0.37	474.67	420
	30	74.40	0.81	1011.33	476
	40	76.53	0.71	926.67	409
	50	86.57	0.88	1262.67	236
	60	84.23	1.87	2664.67	303

CONCLUSION AND FUTURE WORK

The impact of gray hole attacks on the AODV routing protocol is analyzed in this paper.With the help of First order logic the impact of the attacks are clearly understood. Further the graphs also discusses the impact of the attack in detail. During implementing this attack on AODV, the weaknesses of the existing AODV framework are realized. The simulation studies also proved the same. While exploring the AODV, new possibilities for improving its mechanism to withstand against gray hole attack is found. The future work will focus on detecting and preventing other attacks such as collision attack and sink hole attack in MAN ET.

REFERENCES

[1] Haiyun Luo,Fan Ye,Songwu Lu,Lixia Zhang ,"Security in mobile ad hoc networks:challenges and solutions ",Volume :11,Issues:1,PP:38-47,IEEE Journals & Magazines,2004.

[2] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu,Lixia Zhang,Security in Mobile Adhoc Networks:Challenges and Solutions,IEEE Wireless Communications,Feb 2004.

[3] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei,"A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks",Journal of Wirless/Mobile Network Security,Springer 2006.

[4] Buruhanudeen S,"Existing MANET routing protocols and metrics used towards the efficiency and reliability- an overview",PP:231-236,IEEE International Conference on Communications, 2007. ICT- MICC 2007.

[5] H. Yih-Chun, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Ad Hoc Networks, vol. 1,no. 1, page(s): 175 – 192,2003.

[6] P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks Against mobile ad-hoc routing protocols," in In Proceedings of the 4th Annual IEEE Information Assurance Workshop,page(s):60–67, 2003.

[7] H. Yih-Chun, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Adhoc Networks," vol. 1,no. 1, page(s): 175 – 192,2003.

[8] ImadAad,Jean-Pierre Hubaux, Edward W. Knightly,"Impact of Denial of Service Attacks on Ad Hoc Networks,"IEEE/ ACM Transaction on Networking,Vol.16.No.4.August 2008.

[9] Teerawat Issariyakul, Ekram Hossain,"Introduction to Network Simulator NS2", Springer 2009.

[10] C. Perkins, E. Belding-Royer, and S. Das, Ad hoc On-Demand DistanceVector (AODV) Routing, Jul. 2003. IETF RFC 3561(Experimental).

[11] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols,in Proc. 4th Annu. IEEE Inf. Assurance Workshop, Jun.2003, pp. 60–67.

[12] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar,"A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks",IEEE conference on Information and Communications Security,ICICS 2007.

DOI: 03.LSCS.2013.1.532